How Can Organisations Practically Make Microsoft 365 Cyber Resilient and Compliant With DORA & NIS2 Legislation?

2026

Whitepaper

elasticito

risk & threat specialists

Contents

I. Executive Summary

In an increasingly interconnected digital landscape, organisations face constant cyber threats. Traditional security, which focuses only on prevention, is no longer enough. The new standard is cyber resilience, which is an organisation's ability to "anticipate, withstand, recover from, and adapt to adverse cyber events without interrupting its core functions."[1]

This shift is crucial for businesses in the European Union, where new regulations—the Digital Operational Resilience Act (DORA) and the Network and Information Security 2 (NIS2) Directive—mandate a higher level of digital resilience.

Microsoft 365, with its integrated suite of tools (like Microsoft Entra ID, Microsoft Purview, and Microsoft Defender), provides a strong foundation for building this resilience. However, it's vital to understand the shared responsibility model: Microsoft secures the cloud, but the customer is responsible for security in the cloud. This guide outlines how to leverage Microsoft 365 for compliance, identify where third-party solutions may be needed, and build a culture of Continuous Compliance.

INTRODUCTION: NAVIGATING THE EVOLVING CYBER LANDSCAPE

The digital age has brought incredible opportunities but also a complex web of cyber threats. It's no longer a question of if an organisation will be attacked, but when. This reality requires a move from prevention to a more dynamic, adaptive approach: cyber resilience.

DEFINING CYBER RESILIENCE

Cyber resilience goes beyond traditional cybersecurity. It's about an organisation's capacity to adapt to threats and ensure business continuity.

The core pillars of resilience are to:

- **Anticipate:** Understand and prepare for potential threats.
- **Withstand:** Maintain operations during an attack.
- **Recover:** Restore systems and data quickly.
- **Adapt:** Learn from the incident to strengthen future defences.

The Purpose of DORA & NIS2

The EU introduced DORA and NIS2 to protect critical sectors from the widespread disruption that can be caused by ICT-related risks. These regulations are about establishing a common, high level of security to ensure that essential services can withstand and recover from any digital disruption.

> **"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[2]**

-National Institute of Standards & Technology
This proactive mindset is the foundation of DORA and NIS2.

UNDERSTANDING THE EU REGULATORY FRAMEWORKS

DORA and NIS2 are two key pieces of EU legislation designed to strengthen digital resilience. While they share similar goals, their scopes and requirements are distinct yet complementary.

THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

DORA is a comprehensive framework specifically for the financial sector. Its main goal is to harmonise and upgrade existing cyber and IT security regulations, creating a single framework across the EU financial sector. [3]

- **Scope:** Applies to financial entities (banks, investment firms, insurance companies, crypto-asset providers) and their critical ICT third-party service providers (CTPPs), such as cloud providers. [4] This is a major shift, as CTPPs like Microsoft now face direct regulatory scrutiny.
- **Key Pillars:** DORA establishes technical requirements across four key areas:

1. **ICT Risk Management:** Implement a robust framework for identifying, assessing, and managing all ICT risks.
2. **ICT-Related Incident Management and Reporting:** Define and follow a precise process for detecting and reporting incidents. Initial reports for major incidents are due within 24 hours of detection. [5]
3. **Digital Operational Resilience Testing:** Regularly test preparedness through vulnerability assessments and, for significant entities, Threat-Led Penetration Testing (TLPT).
4. **Managing ICT Third-Party Risk:** Bear full responsibility for compliance even when using third-party providers. A key requirement is maintaining a Register of Information (RoI) detailing all contractual arrangements.

THE NETWORK & INFORMATION SECURITY DIRECTIVE (NIS2)

NIS2 is the EU's updated cybersecurity framework. It replaces the original NIS Directive and expands its scope to a wider range of critical sectors deemed "essential" or "important" to the economy and society. [6]

- **Scope:** Covers sectors like energy, transport, health, digital infrastructure, and digital services (including cloud computing providers).
- **Key Pillars:** NIS2 introduces strengthened requirements across four areas:

1. **Cybersecurity Risk Management Measures:** Adopt technical and organisational measures to manage risks, including policies for risk analysis, business continuity, supply chain security, and the use of cryptography.
2. **Corporate Accountability:** Senior management is now held accountable for overseeing cybersecurity measures, with the potential for personal liability for non-compliance.
3. **Incident Reporting Obligations:** Promptly report significant incidents, with an "early warning" due within 24 hours of awareness. [7]
4. **Business Continuity:** Maintain robust plans, including up-to-date backups and disaster recovery.

FOUNDATIONS OF CYBER RESILIENCE WITH MICROSOFT 365

Building a strong cyber resilience posture requires a strategic approach built on foundational principles. Microsoft 365 provides a powerful ecosystem to support this.

THE ZERO TRUST MODEL

The Zero Trust security model is the cornerstone of modern security. Its core principle is "never trust, always verify."[8] Every access request must be explicitly verified, regardless of its origin.

Key Tenets:

- **Verify explicitly:** Authenticate and authorise based on all available data points.
- **Use least privilege access:** Grant only the necessary permissions.
- **Assume breach:** Continuously monitor for potential compromises.

Microsoft's security solutions, like Microsoft Entra ID, are built on these principles. Adopting a Zero Trust architecture is not just a best practice: it's a strategic enabler for complying with DORA and NIS2.

MICROSOFT'S 5 MINIMUM STANDARDS

Microsoft's analysis shows that most attacks succeed due to a lack of basic security hygiene.

The company proposes five minimum standards that can protect organisations from roughly **98%** of common attacks: [9]

- **Enable Multi-Factor Authentication (MFA):** A critical layer of security to protect against compromised credentials.
- **Apply Zero Trust Principles:** Limit the impact of a breach by verifying all access.
- **Use Modern Anti-Malware:** Implement Extended Detection and Response (XDR) to automatically block attacks.
- **Keep Up to Date:** Ensure all systems are patched and updated.
- **Protect Data:** Know where important data is and protect it with appropriate systems.

ACHIEVING DORA COMPLIANCE WITH MICROSOFT 365

Microsoft 365 offers a comprehensive suite of tools to help organisations meet DORA's stringent requirements.

ICT Risk Management

Governance & Control:

Microsoft Entra ID enforces least privilege access and provides Conditional Access policies. Microsoft Purview offers a central governance model to gain visibility into your data estate.[10]

Risk Assessment:

Microsoft Defender for Cloud helps identify and assess risks, providing a "secure score" to improve your posture. Microsoft Sentinel offers a cloud-native SIEM (Security Information and Event Management) for real-time threat analysis.

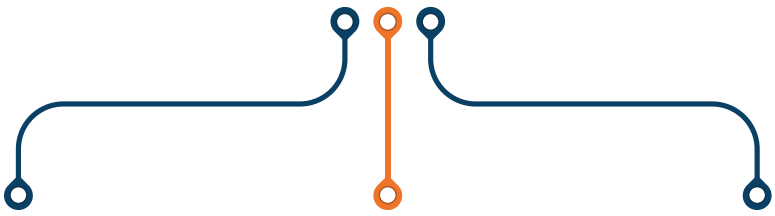
Data Protection:

Microsoft Purview provides Data Loss Prevention (DLP) and Information Protection to classify, encrypt, and protect sensitive data.

Business Continuity:

Microsoft 365 services like SharePoint and OneDrive offer inherent resilience with geo-redundancy and versioning. They are engineered to support business continuity, but customers must actively implement and test these features.

Incident Management & Reporting



Detection & Analysis

Microsoft Defender XDR provides a unified view of threats across endpoints, identities, and applications. Microsoft Sentinel excels at correlating security events to generate alerts for immediate investigation.

Response

Defender XDR offers automated response capabilities, while Sentinel's SOAR (Security Orchestration, Automation, and Response) playbooks can trigger automated remediation.

Reporting

Microsoft Purview Audit logs thousands of user and administrator operations, providing the detailed records needed for DORA's strict reporting timelines (24-hour initial report).

Digital Operational Resilience Testing

Threat-Led Penetration Testing (TLPT):

For significant financial entities, DORA mandates TLPT every three years. This goes beyond basic testing and requires an organisation to actively validate its ability to withstand a real attack. This will likely require specialised external services.

Testing Program:

Microsoft Purview Compliance Manager helps you manage compliance requirements and report to auditors.

Managing ICT Third-Party Risk

Evaluation:

Organisations must maintain a Register of Information (RoI) detailing all contractual arrangements with third parties.

Contractual Arrangements:

Microsoft offers a specific DORA contract addendum to supplement existing agreements, providing transparency on subcontractors and addressing third-party risk

Exit Strategies:

DORA requires organisations to have exit strategies in case of provider failure. This encourages diversification rather than reliance on a single provider.

ACHIEVING NIS2 COMPLIANCE WITH MICROSOFT 365

NIS2 sets a high bar for cybersecurity across a broad range of critical sectors. Microsoft 365 provides a strong foundation for meeting these requirements.

Cybersecurity Risk Management

Risk Analysis & Security Policies:

Microsoft Defender for Cloud provides continuous security assessments and recommendations. Azure Policy offers built-in initiatives to enforce security standards at scale.

Incident Handling:

Microsoft Defender XDR and Microsoft Sentinel enable robust, real-time incident detection and response.

Encryption:

Microsoft 365 services use encryption by default. Microsoft Purview Information Protection allows you to classify and encrypt sensitive data using sensitivity labels.

Cyber Hygiene & Training:

Microsoft Entra ID is essential for enforcing MFA, password protection, and least-privilege access. Microsoft Defender for Office 365 provides anti-phishing training to educate users. The human factor is a key part of NIS2, and technology alone is not enough.

Corporate Accountability

Management Oversight:

NIS2 places accountability on senior management. The Microsoft Purview Compliance Manager provides a centralised view of compliance, helping leaders manage and report on their security posture.

Incident Reporting Obligations

Prompt Reporting:

NIS2 requires an "early warning" within 24 hours of a significant incident. Microsoft Sentinel is designed to facilitate this with real-time alerts and automated workflows, ensuring you can meet these strict deadlines.

Business Continuity & Supply Chain Security

Business Continuity:

NIS2 requires up-to-date backups. While Microsoft 365 offers strong native resilience features, its backup and retention capabilities have limitations. This creates a "backup gap" for organisations with long-term retention needs.

Supply Chain Security:

Organisations must conduct regular risk assessments of their suppliers. Microsoft commits to security measures in its contracts, which helps customers meet these obligations.

THE SHARED RESPONSIBILITY MODEL & COMPLIANCE GAPS

While Microsoft 365 is a powerful platform, a crucial principle to remember is the shared responsibility model. Microsoft is responsible for the security of the cloud, but the customer is responsible for security in the cloud. [11]

- **Microsoft's Role:** Securing the underlying infrastructure (datacentres, network).
- **Customer's Role:** Managing data, applications, identities, and configurations.

This means you cannot assume "out-of-the-box" compliance. You must actively configure and manage these tools.

ADDRESSING THE BACKUP GAP

A significant limitation of native Microsoft 365 is its backup and retention functionality. The native recycle bin retains deleted items for only 93 days, which is often not enough for regulatory requirements that may mandate 6-7 years of retention. This requires implementing third-party backup solutions to ensure true data resilience and compliance.

SHADOW IT & UNMANAGED DATA

The rise of remote work has led to "shadow IT" and unmanaged data in personal accounts and unapproved third-party apps. This data lacks proper security, backup, and governance, creating a major compliance risk. DORA and NIS2's emphasis on comprehensive risk management means you must have visibility and control over all data, regardless of where it resides.

IMPLEMENTING A CONTINUOUS COMPLIANCE AND RESILIENCE FRAMEWORK

Compliance with DORA and NIS2 is an ongoing journey, not a one-time project. It requires a shift from static, audit-driven security to a proactive, continuous culture of vigilance.

Compliance with DORA & NIS2

- Continuous Monitoring: Use tools like Microsoft Sentinel and Purview Audit for 24/7 monitoring and logging. This allows you to demonstrate continuous effectiveness of your controls, not just a snapshot in time.
- Regular Testing: Integrate regular audits and penetration tests into your processes to identify weaknesses and validate controls.
- Post-Incident Review: Both regulations require you to learn from incidents. Analyse root causes and implement corrective measures to prevent recurrence.

10 STEPS TO MICROSOFT 365 CYBER RESILIENCE

STEP	DESCRIPTION OF THE STEP	RELEVANT MICROSOFT 365 SERVICE/FEATURE
1. Multi-factor Authentication (MFA)	Implement MFA for all users.	Microsoft Entra ID
2. Least-Privilege Access	Grant users the minimum permissions needed.	Microsoft Entra ID (PIM, Conditional Access), Microsoft Intune (EPM)
3. Regular Backups	Implement a comprehensive backup strategy for all critical data.	Third-party backup solutions
4. Immutable Backups	Ensure backups cannot be altered or deleted.	Third-party backup solutions
5. Incident Response Plan	Develop and regularly test a plan for incidents.	Microsoft Defender XDR, Microsoft Sentinel, Microsoft Purview Audit
6. Regular Audits and Penetration Testing	Conduct frequent security audits and tests.	Microsoft Defender for Cloud, external TLPT services
7. Software Restriction Policies	Control which software can run on devices.	Microsoft Intune
8. Monitoring and Logging	Continuously monitor network and system activity.	Microsoft Sentinel, Microsoft Purview Audit
9. Data Separation	Logically separate sensitive data from less critical data.	Microsoft Purview Information Protection
10. Encryption	Encrypt data at rest and in transit.	Microsoft 365 services, Microsoft Purview Information Protection

CONCLUSION: A PROACTIVE PATH TO DIGITAL RESILIENCE

DORA and NIS2 represent a significant shift in the regulatory landscape, but they also provide a clear roadmap for building true cyber resilience. By strategically leveraging Microsoft 365's powerful capabilities, you can not only meet these stringent requirements but also build a more secure and resilient organiSation.

Remember that this journey is ongoing. Embrace a Zero Trust mindset, address the backup gap with third-party solutions, and foster a continuous compliance culture. By combining powerful technology with disciplined processes, you can protect your operations, data, and reputation in the face of an ever-evolving threat landscape.

Works Cited

1. HPE. "What is Cyber Resilience? | Glossary | HPE." Accessed August 13, 2025.
2. NIST. "cyber resiliency - Glossary | CSRC - NIST Computer Security Resource Center." Accessed August 13, 2025.
3. AMF. "The Regulation on Digital Operational Resilience in the Financial Sector (DORA) - AMF." Accessed August 13, 2025.
4. DLA Piper. "DORA: The Digital Operational Resilience Act - DLA Piper." Accessed August 13, 2025.
5. Two Birds. "NIS2 Directive." Accessed August 13, 2025.
6. Microsoft. "What is DORA? - DORA | Microsoft Learn." Accessed August 13, 2025.
7. Oracle. "Oracle Cloud Compliance." Accessed August 13, 2025.
8. Entrust. "Understanding the Digital Operational Resilience Act (DORA) - Entrust." Accessed August 13, 2025.
9. Microsoft. "Cyber resilience | Microsoft Security." Accessed August 13, 2025.
10. Microsoft. "SharePoint and OneDrive data resiliency in Microsoft 365 - Microsoft." Accessed August 13, 2025.
11. Arcserve. "The Microsoft 365 Backup Gap: Your Role in Securing Business Data - Arcserve." Accessed August 13, 2025.

elasticito
risk & threat specialists

Let Elasticito's team of cyber risk experts handle your vendor risk assessments

We have not yet come across a cyber risk or information security team that is not under-resourced and has time on their hands. Assessing third parties for the cyber risks that they might pose to your business is a critical, but additional task to add to the already full job-list of security and risk teams.

We combine the use of world-class technology tools and our team of cyber risk specialists to streamline the assessment and monitoring of vendor cyber risk assessments so that our customers can focus on delivering value back to their business stakeholders through accurate and up to date vendor cyber risk metrics.

+44 (0) 3330428268 information@elasticito.com www.elasticito.com